HIPAA – Health Insurance Portability & Accountability Act and the Privacy Act

MSgt Nechele M. Chambers
Senior Enlisted Liaison
TRICARE Area Office-Europe

Agenda

- HIPPA
  - Privacy Rule
  - Security Rule
  - Key Components
  - Authorizations
  - Data Stewardship
- Privacy Act of 1974

Health Insurance Portability & Accountability Act (HIPPA)

- In August 1996, President Clinton signed into law the Public Law 104-91, Health Insurance Portability and Accountability Act (HIPAA). The Act included provisions for health insurance portability, fraud and abuse control, tax related provisions, group health plan requirements, revenue offset provisions, and administrative simplification requirements.

- Purpose: To improve the portability of health insurance coverage; combat waste, fraud and abuse; and simplify health care administration.

- The Military Health System (MHS) must comply with the requirements of HIPAA, both as a provider of health care - through the Military Treatment Facilities - and as the TRICARE health plan - through contracted network health care services.

HIPPA Privacy Rule

The HIPAA Privacy Rule institutes business processes to protect the use and disclosure of protected health information (PHI). PHI is individually identifiable health information, including demographics, in paper, electronic, or oral form. PHI is not limited to the documents contained in the official medical record. The HIPAA Privacy Rule allows the use and disclosure of PHI for treatment, payment and health care operations without written authorization from the patient. Other uses and disclosures require permission. The compliance date for the HIPAA Privacy rule was April 14, 2003.

HIPPA Security Rule

The HIPAA Security Rule is designed to provide protection for all individually identifiable health information that is maintained, transmitted or received in electronic form—not just the information in standard transactions. All covered entities were to be in compliance with the HIPAA Security Rule no later than April 20, 2005. The safeguards in the HIPAA Security Rule are divided into three categories: Administrative Safeguards; Physical Safeguards; and Technical Safeguards.

Specific information regarding HIPAA Privacy and Security can be found on the TMA Privacy Office Web site at www.tricare.osd.mil/tmaprivacy.

Key Components

Comprises three rules:

1. Transactions and Code Sets; Security
   - *Transparent to beneficiaries; technical aspects related to transmission of health data – standardizes data packets*
2. Privacy
   - *Very Important to the Beneficiary and to POCs*
3. HIPAA Privacy establishes standards on the use and disclosure of protected health information (PHI)

Authorizations

- Covered entities must obtain an individual's authorization before using or disclosing PHI for purposes other than treatment, payment or healthcare operations.
- Authorization is not required for:
  - *Filling prescriptions*
  - *Referrals to Specialists*
  - *Communicate treatment Options*
- To use or disclose PHI on a spouse or family member, an authorization must be obtained from the person whose PHI is required.

Data Stewardship

- Sensitive Date
- Your Trusted Position
- Basic Guidance
- Ways to Safeguard Data

Sensitive Data

- Medical Record: Any item or collection of items of personally identifiable information maintained in any form by DoD regarding the provision of healthcare. These can include:
  - *Paper or electronic records in an information system;*
  - *Files with personally identifiable information on a PC*
- Information attained from medical records/claims data that contains either personally identifiable information or
- Data about healthcare in a manner that would allow one to deduce a person's identity.

Your Trusted Position

When you are appointed as a TRICARE POC, you are responsible for maintaining the safety and confidentiality of the patient information to which you now have access!

Ways to Safeguard

- Do not discuss patient information with those who do not need to know.
- Ensure privacy if you need to discuss patient information.
- Password protect all data.
- Never leave terminal unattended when displaying sensitive data.
- Bottom Line – ***Treat patient Information as you would Classified information!***

Privacy Act of 1974

Establishment of “Fair Information Practices”

- Proactive protection of sensitive information
- Allowed release of non-sensitive information

Criminal and Administrative Penalties and fines up to $5,000 for violations

- Improper release of data
- Information must be safeguarded!

QUESTIONS